| NODIS Library | Program Management(8000s) | Search |

NASA Procedural Requirements

COMPLIANCE IS MANDATORY

NPR 8705.5A
Effective Date: June 07, 2010
Expiration Date: June 07, 2015

Printable Format (PDF)

Request Notification of Change (NASA Only)

Subject: Technical Probabilistic Risk Assessment (PRA) Procedures for Safety and Mission Success for NASA Programs and Projects

Responsible Office: Office of Safety and Mission Assurance

| TOC | Preface | Chapter1 | Chapter2 | Chapter3 | Chapter4 | Chapter5 | Appen
AppendixA | AppendixB | AppendixC | ALL |

Chapter 2. PRA Process

2.1 Overview

2.1.1 The process for conducting a PRA is shown in Figure 1. This process starts with the definition of objectives and ends with the documentation of the results. Deviations from the process and techniques summarized below may be necessary based on the objectives and scope of the PRA. These deviations need to be approved before implementation.

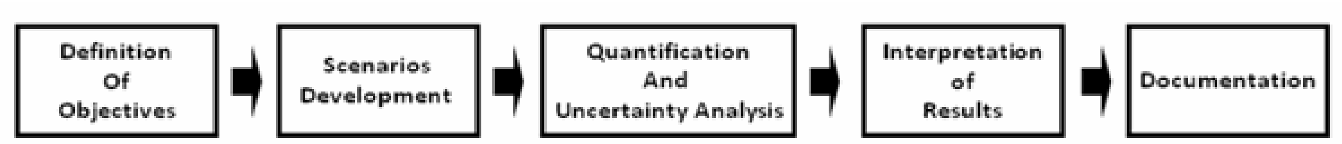

Figure 1. PRA Process

2.2 Definition of PRA Objective(s)

2.2.1 The program/project manager shall:

a. Ensure that a PRA is conducted for: (i) payloads with a risk classification level of A, as defined in NPR 8705.4 (Requirement 69148);(ii) Category I programs/projects as defined in NPR 7120.5(Requirement 69149);(iii) any other program or project determined by the program manager to meet the criteria of Priority Ranking I programs/projects as defined in NPR 8715.3 (Requirement 69150).

b. Determine whether a PRA is necessary for: (i) Priority Ranking II programs/projects as identified in Chapter 2 of NPR 8715.3, NASA General Safety Program Requirements (Requirement 69152)

; and (ii) payloads with a risk classification level of B, as defined in NPR 8705.4, Risk Classification for NASA Payloads (Requirement 69153).

c. Request concurrence from the SMA Technical Authority if the determination is made (see paragraph 2.2.1.b) that a PRA is not necessary for (i) Priority Ranking II programs/projects as identified in Chapter 2 of NPR 8715.3, NASA General Safety Program Requirements (Requirement 69155)

; and (ii) payloads with a risk classification level of B, as defined in NPR 8705.4, Risk Classification for NASA Payloads (Requirement 69156).

d. Define the objective(s) of the PRA and its intended applications to support decisions and technical reviews for selected life-cycle phases (Requirement 69157).

Note: The objectives and intended applications provide information needed to define the scope, level of detail, schedule, and end states (performances measures) of the PRA which are based on the program/project life-cycle phase and the decisions being supported prior to and during a specific technical review.

e. Decide the uses (and life-cycle phases) that are supported by a PRA for existing programs/projects (Requirement 69159).

2.2.2 The PRA lead shall:

a. Describe the scope and level of detail of the PRA, including the identification of end-states (undesirable consequences, performance measures, figures of merit) of interest, which are consistent with the PRA objectives and applications defined in paragraph 2.2.1 of this NPR and documented in the approved PRA plan (Requirement 33035). (See Chapter 3 of this NPR.)

b. Define quantitative performance measures and numerical criteria that are evaluated by the PRA consistent with the objectives and application defined in the approved PRA plan (Requirement 69148).

c. Develop a PRA schedule compatible with the objectives, applications, and life-cycle phases identified by the program/project manager (Requirement 69163).

2.3 PRA Requirements

2.3.1 The type of information required and the types of scenarios modeled will vary during the assessment of each program/project life-cycle phase dependent on the decisions supported and the associated technical reviews and Key Decision Points (KDP) (see NPR 7123.1A, NASA Systems Engineering Process and Requirements). Some deviation from the results summarized below may be necessary as long as the PRA meets program/project safety and health objectives.

2.3.2 The PRA lead shall conduct a systematic and comprehensive PRA applicable to the decisions and program/project life-cycle phase being supported that includes definition of objectives, scenario development, quantification and uncertainty analysis, interpretation of results, and documentation consistent with the approved PRA plan (Requirement 69166).

2.4 Scenario Development

2.4.1 An accident scenario starts with an initiating event and progresses through a series of successes or failures of intermediate events leading to a defined end state. A PRA attempts to identify and quantify all applicable scenarios. The identification of the scenarios involves a thorough understanding of the decisions being supported and the program/project concepts, architecture, systems, and operations to be modeled including the success states (conditions or parameters for success) needed to fulfill mission objectives; the identification of the initiating events that mark the beginning of the accident scenarios; and an understanding of the failure causes (or their complements, successes) of each event in the accident scenarios. (See the Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners)

2.4.2 Consistent with the objectives and application defined in the approved PRA plan, the PRA lead shall:

a. Define the concept, mission, architecture, system, and/or operation, including the identification and definition of applicable mission success criteria, being assessed to support specific decisions and life-cycle phase(s) (Requirement 69170).

Note: The information needed to describe the design and operation of the system may consist of Baseline Concept Documents, functional descriptions, operating manuals, drawings, schematics, parts lists, materials, hardware maps, specifications, and interface descriptions. Existing data/products should be utilized whenever possible to avoid duplication of effort and ensure product consistency. If little or no documentation is available to perform scenario and failure modeling, the analyst not familiar with the technology will need to interview engineers and operating crews supporting the design for the project to ensure an understanding of how the system is intended to be or being operated. In this case, the best possible description that can be developed for design and operation based on interview notes can be used for the analysis.

b. Identify and describe the contributing set of initiating events that were used to initiate accident scenarios leading to the defined end states (Requirement 69172) including:

(1) The initiating events that are not included in the assessment and the rationale for exclusion (Requirement 69173).

(2) Any initiating events that are treated as a group, their group initiator frequencies, and the techniques used to derive the group initiator frequencies (Requirement 69174).

Note: See Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners.

c. Identify and describe the accident scenarios leading to the defined end states including the initiating events, intermediate events, and contributing conditions (Requirement 69176) including:

Note: The review of applicable Hazard Analyses and Failure Mode and Effects Analyses can be used to identify accident contributors and accident scenarios. In those cases where the Hazard Analysis is not complete or available, the PRA analyst can interview safety engineers, design engineers and operations personnel to identify a list of possible hazards. In those cases where these analyses are not complete or available, the PRA analyst can interview reliability engineers, design engineers and operating crews to identify a list of possible failure modes that may impact safety and health, and mission success.

(1) The models and techniques used to identify the accident scenarios (Requirement 69178).

(2) The phenomenological variables and the timing or event sequencing modeled (Requirement 69179).

Note: Phenomenological variables are those parameters used to characterize the scenario being evaluated or modeled, such as knowing the size of the orbital debris hitting the vehicle, the radiation levels, and the strength of materials, fluid pressure, and fluid temperature.

d. Identify and describe the analytical techniques (reliability and failure models) used to assess the accident scenario event probabilities including their failure causes (Requirement 69181).

2.5 Quantification and Uncertainty

2.5.1 Quantification refers to the process of evaluating the probability (or frequency) and the severity of the consequences associated with the end states. The frequency of occurrence of each end state is the logical product of the initiating event frequency and the (conditional) probabilities of the intermediate event along the scenario path from the initiating event to the end state. Quantification involves the collection and analysis of data and information in order to estimate various parameters of the PRA model, including event probabilities and consequence severities, and the treatment of uncertainty (both aleatory and epistemic) in these parameters and the overall results. Uncertainty analysis captures both the randomness in physical processes and the uncertainty in knowledge of the processes, models, and parameters used in the analysis. (See the Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners)

2.5.2 Consistent with the objectives and application defined in the approved PRA plan, the PRA lead shall:

a. Quantify the probability, including uncertainty, for each event in the accident scenario described in paragraphs 2.4 above (Requirement 69185).

b. Quantify the probability, including uncertainty, for the individual accident scenarios (Requirement 69185).

c. Quantify the total probability, including uncertainty, for each defined end state (summed from all the accident scenarios leading to the same end-state) (Requirement 69187).

d. Quantify the severity of the end states (if the magnitude of the end state can be quantified) including the uncertainty in end state severity (Requirement 69188).

e. Describe the data used in quantifying event probabilities and end state severities (Requirement 69189).

f. Describe the techniques used to propagate the uncertainty in the scenario probabilities and the end state severities (Requirement 69190).

g. Quantify the uncertainty (accounting for both aleatory and epistemic uncertainties) for all of the probabilities and severities evaluated in the PRA including the effects of sensitivity assessments (Requirement 69191).

Note: Aleatory uncertainty is the natural, unpredictable variation (randomness) in the performance of the system or physical processes being studied. Epistemic uncertainty is due to a lack of knowledge about the processes, models, parameters, and behavior used in the analysis.

h. Seek the expertise needed to reduce the epistemic uncertainty to as low an uncertainty as practical (Requirement 69193).

i. Provide an ordering and description of the major contributors covering events, accident scenarios, and end states (Requirement 69194).

Note: Importance measures can be used to identify major contributors to risk. If these measures are used, the results should be described in the risk assessment report.

2.6 Interpretation of the PRA Results

2.6.1 The results of the PRA process are interpreted for application to specific decisions that occur during a program/project life-cycle phase and used to support technical reviews. Some applications may include the identification of mission concepts and architectures with minimum risk while other applications may include the design and/or operation of specific systems and/or mission profiles. Key points in interpreting PRA results include the analysis objectives and scope, limitation and assumptions in the analysis and their impact on the results, data used, uncertainty, and the influence of the models (e.g., common-cause, human reliability, software reliability, phenomenological) on the overall results.

2.6.2 Consistent with the objectives and application defined in the approved PRA plan, the PRA lead shall:

a. Provide an interpretation of the results applicable to the PRA objectives, scope, specific decision(s), and life-cycle phase(s) being supported (Requirement 69199).

b. Explain the overall degree of uncertainty about the results and provide a discussion of the sources of uncertainty (Requirement 69200).

c. Describe the applicability, limitations, and strengths of the PRA to support and inform decisions and trades (Requirement 69201).

Note: The applicability, limitation, and strengths of the PRA to support decisions during an applicable technical review should be described.

2.7 PRA Documentation

2.7.1 PRA documentation includes the PRA results, models, data, and supporting information and is maintained under configuration control. Documentation can be in the form of a summary report and records of detailed supporting models, data, analyses, and information.

2.7.2 Consistent with the objectives and application defined in the approved PRA plan, the PRA lead shall:

a. Produce and maintain a report of the PRA that supports the decisions associated with the specified program/project life-cycle phase and technical review (Requirement 69206

including:

(1) the results given in paragraphs 2.3 through 2.6, above,

(2) the analysis and modeling assumptions,

(3) the treatment of explicit dependencies, event correlations, and common cause failure modeling,

(4) the integration of specialized and off-line analyses,

(5) model integration,

(6) the principal results obtained including decisions and trade-offs supported, and

(7) the principal conclusions.

b. Ensure that the detailed PRA models developed, data used, analyses carried out, computer printouts generated, results obtained, and all relevant supporting information are available (Requirement 692621

.

c. Develop a presentation package giving the scope, assumptions, and key results for communication purposes (Requirement 69262).

2.7.3 The program/project manager shall have the authority to approve of the public release of the summary PRA report and access to the supporting models, data, analyses, and information (Requirement 69263)

.

2.8 PRA Quality

2.8.1 For all PRAs, consistent with the objectives and application defined in the approved PRA plan, the PRA lead shall ensure that the PRA follows quality assurance principles and practices that are analogous to those in other engineering fields including:

a. Assurance of the accuracy, rigor, fidelity, and completeness of the models, scenarios, and data analyses, so that reported results are applicable to the decisions and technical reviews supported (Requirement 69266)

.

b. The comparison of quantitative results with heritage data for similar systems, subsystems, or components when available (Requirement 69267)

.

c. Use of accepted and justified methods, analytical techniques, and tools that fit the specific application (Requirement 69268)

.

d. Use of validated software with version control and baseline documentation (Requirement 69269)

.

Note: Validated software has been reviewed and benchmarked for the application for which it is being used with documentation that includes a user manual and code description.

e. Maintenance and updating of models as the PRA effort progresses (Requirement 69271)

.

f. Establishment of strong ties with program/project configuration and requirements management activities and operations personnel to ensure that the PRA being developed reflects the latest or the most suitable design (Requirement 69272)

.

g. The use of terminology in the PRA that is consistent with what is used in the program/project in order to facilitate risk communication (Requirement 69173).

Note: Use consistent terminology for all significant factors that might cause or affect the outcome of an undesired event. Examples include the names of initiating events, mitigating systems, and components.

| TOC | Preface | Chapter1 | Chapter2 | Chapter3 | Chapter4 | Chapter5 | Appen
AppendixA | AppendixB | AppendixC | ALL |

| NODIS Library | Program Management(8000s) | Search |

DISTRIBUTION:
NODIS